The Power of Basis Selection in Fourier Sampling: Hidden Subgroup Problems in Affine Groups

Cristopher Moore
University of New Mexico
moore@cs.unm.edu

Daniel Rockmore
Dartmouth College
rockmore@cs.dartmouth.edu

Alexander Russell
University of Connecticut
acr@cse.uconn.edu

Leonard J. Schulman
CalTech
schulman@caltech.edu

Abstract

Many quantum algorithms, including Shor's celebrated factoring and discrete log algorithms, proceed by reduction to a *hidden subgroup problem*, in which a unknown subgroup H of a group G must be determined from a quantum state ψ over G that is uniformly supported on a left coset of H. These hidden subgroup problems are typically solved by *Fourier sampling*: the quantum Fourier transform of ψ is computed and measured. When the underlying group is nonabelian, two important variants of the Fourier sampling paradigm have been identified: the *weak standard method*, where only representation *names* are measured, and the *strong standard method*, where full measurement (i.e., the row and column of the representation as well as its name) occurs. It has remained open whether the strong method is indeed stronger, that is, whether there are hidden subgroups that can be reconstructed via the strong method but *not* by the weak, or any other known, method.

In this article, we settle this question in the affirmative. We show that hidden subgroups of semidirect products of the form $\mathbb{Z}_q \ltimes \mathbb{Z}_p$, where $q \mid (p-1)$ and $q = p/\mathrm{polylog}(p)$, can be efficiently determined by the strong standard method. Furthermore, the weak standard method and the "forgetful" abelian method are insufficient for these groups so that, in fact, it appears that use of the corresponding nonabelian representation theory is crucial. We extend this to an information-theoretic solution for the hidden subgroup problem over the groups $\mathbb{Z}_q \ltimes \mathbb{Z}_p$ where $q \mid (p-1)$ and, in particular, the affine groups A_p. Finally, we prove a simple closure property for the class of groups over which the hidden subgroup problem can be solved efficiently.

Copyright © 2004 by the Association for Computing Machinery, Inc. and the Society for industrial and Applied Mathematics. All Rights reserved. Printed in The United States of America. No part of this book may be reproduced, stored, or transmitted in any manner without the written permission of the publisher. For information, write to the Association for Computing Machinery, 1515 Broadway, New York, NY 10036 and the Society for Industrial and Applied Mathematics, 3600 University City Science Center, Philadelphia, PA 19104-2688

1 The hidden subgroup problem

One of the principal quantum algorithmic paradigms is the use of the abelian Fourier transform to discover a function's hidden periodicities. In the examples relevant to quantum computing, a function h defined on an abelian group G has "hidden periodicity" if there is a "hidden" subgroup H of G so that h is precisely invariant under translation by H or, equivalently, h is constant on the cosets of H and takes distinct values on distinct cosets. The *hidden subgroup problem* is the problem of determining the subgroup H from such a function. Algorithms for these problems typically adopt the approach detailed below, called *Fourier sampling* [2]:

Step 1. Prepare two registers, the first in a uniform superposition over the elements of a group G and the second with the value zero, yielding the state

$$\psi_1 = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |0\rangle \ .$$

Step 2. Calculate the (classical polynomial-time) function h defined on G and XOR it with the second register. This entangles the two registers and results in the state

$$\psi_2 = \frac{1}{\sqrt{|G|}} \sum_{g \in G} |g\rangle \otimes |h(g)\rangle \ .$$

Step 3. Measure the second register. This produces a uniform superposition over one of h's level sets, i.e., the set of group elements g for which $h(g)$ takes the measured value h_0. As the level sets of h are the cosets of H, this puts the first register in a uniform distribution over superpositions on one of those cosets, namely cH where $h(c) = h_0$. Moreover, it disentangles the two registers, resulting in the state

$$\psi_3 = \frac{1}{\sqrt{|H|}} \sum_{h \in H} |ch\rangle \otimes |h_0\rangle \ .$$

Step 4. Compute the Fourier transform of ψ_3 and measure the result.

For example, in Simon's algorithm [22] for the "XOR-mask" oracle problem, the "ambient" group G over which the Fourier transform is performed is $\mathbb{Z}_2^n$, and H is a subgroup of order 2. In Shor's factoring algorithm [21] G is the group $\mathbb{Z}_n^*$ where n is the number we wish to factor, $h(x) = r^x \bmod n$ for a random $r < n$, and H is the subgroup of $\mathbb{Z}_n^*$ of index order(r). (However, since $|\mathbb{Z}_n^*|$ is unknown, Shor's algorithm actually performs the transform over $\mathbb{Z}_q$ where q is polynomially bounded by n; see [21] or [8, 9].)

These are all abelian instances of *hidden subgroup problems* (HSPs). Interest in *nonabelian* versions of the HSP evolved from the relation to the elusive Graph Automorphism problem: it would be sufficient to solve efficiently the HSP over the permutation group S_n in order to have an efficient quantum algorithm for graph automorphism (see, e.g., Jozsa [13] for a review). This was the impetus behind the development of the first nonabelian quantum FFT [1] and is, to a large degree, the reason that the nonabelian HSP has remained such an active area of research in quantum algorithms.

In general, we will say that the HSP for a family of groups has a *Fourier sampling* algorithm if a procedure similar to that outlined above works. Specifically, the algorithm prepares a superposition of the form

$$\frac{1}{\sqrt{|H|}} \sum_{h \in H} |ch\rangle,$$

where H is the hidden subgroup of G and c is an element selected at random from G (cf. Step 3 above), computes the (quantum) Fourier transform of this state, and measures the result. After a polynomial number of such trials, a polynomial amount of classical computation, and, perhaps, a polynomial number of classical queries to the function h to confirm the result, the algorithm produces a set of generators for the subgroup H with high probability. When G is abelian, the notion of "measuring" the resulting (Fourier transformed) state has a clear meaning: one observes the "frequency" χ with probability equal to the squared magnitude of the transform at that frequency. In the case where the transform is taken over a non-abelian group, however, it is necessary to select bases for each representation of G to perform full measurement. (This is explained in more detail in the sequel.) The relationship of this choice of basis to the information gleaned from the measurement is the subject of this article.

Since we are typically interested in exponentially large groups, we will take the size of our input to be $n = \log |G|$. Throughout, "polynomial" means polylogarithmic in the size of the group.

Nonabelian HSPs: History and Context. Though a number of interesting results have been obtained on the nonabelian HSP, the groups for which efficient solutions are known remain woefully few and sporadic. On the positive side, Roetteler and Beth [18] give an algorithm for the wreath product $\mathbb{Z}_2^k \wr \mathbb{Z}_2$. Ivanyos, Magniez, and Santha [12] extend this to the more general case of semidirect products $K \ltimes \mathbb{Z}_2^k$ where K is of polynomial size, and also give an algorithm for groups whose commutator subgroup is of polynomial size. Friedl, Ivanyos, Magniez, Santha and Sen solve a problem they call Hidden Translation, and thus generalize this further to what they call "smoothly solvable" groups: these are solvable groups whose derived series is of constant length and whose abelian factors are each the direct product of an abelian group of bounded exponent and one of polynomial size [5]. (See also Section 5.)

In another vein, Ettinger and Høyer [3] show that the HSP is solvable for the dihedral groups in an *information-theoretic* sense; namely, a polynomial number of quantum queries to the function oracle gives enough information to reconstruct the subgroup, but the best known reconstruction algorithm takes exponential time. More generally, Ettinger, Høyer and Knill [4] show that for *arbitrary* groups the HSP can be solved information-theoretically with a finite number of quantum queries, but do not give an explicit set of measurements to do so.

Our current understanding of the HSP, then, divides group families into three classes.

I. Fully Reconstructible. Subgroups of a family of groups $\mathbf{G} = \{G_i\}$ are *fully reconstructible* if the HSP can be solved with high probability by a quantum circuit of size polynomial in $\log |G_i|$.

II. Information-Theoretically Reconstructible. Subgroups of a family of groups $\mathbf{G} = \{G_i\}$ are *information-theoretically reconstructible* if the solution to the HSP for G_i is determined information-theoretically by the fully measured result of a quantum circuit of size polynomial in $\log |G_i|$.

III. Quantum Information-Theoretically Reconstructible. Subgroups of a family of groups $\mathbf{G} = \{G_i\}$ are *quantum information-theoretically reconstructible* if the solution to the HSP for G_i is determined by the quantum state resulting from a quantum circuit of polynomial size in $\log|G_i|$, in the sense that there is a POVM that yields the subgroup H with constant probability. (Note that there is no guarantee that this POVM can be implemented by a small quantum circuit.)

In each case, the quantum circuit has oracle access to a function $h : G \to S$, for some set S, with the property that f is constant on each left coset of a subgroup H, and distinct on distinct cosets.

In this language, then, the result of [4] shows that subgroups of arbitrary groups are quantum information-theoretically reconstructible, whereas it is known that subgroups of abelian groups are in fact fully reconstructible. The other work cited above has labored to place specific families of (nonabelian) groups into the more algorithmically meaningful classes I and II above.

All the above results use the abelian Fourier transform, even in the cases in which the groups of interest are nonabelian; it turns out that each of these groups are "close enough" to abelian that a "forgetful" abelian Fourier analysis, which treats the groups as though their multiplication rule was commutative, suffices to detect subgroups. Nevertheless, as we shall see, there are situations in which abelian Fourier analysis does not suffice and, instead, the full power of the nonabelian Fourier transform associated with the group is required.

Fourier analysis over a finite abelian group A proceeds by expressing a function $f : A \to \mathbb{C}$ as a linear combination of special functions $\chi : A \to \mathbb{C}$ which are *homomorphisms* of A into $\mathbb{C}$. If $A = \mathbb{Z}_p$, for example, the homomorphisms from A to $\mathbb{C}$ are the familiar basis functions $\chi_t : z \mapsto \mathrm{e}^{2\pi i t z/p} \equiv \omega_p^{tz}$, where $\omega_p = \mathrm{e}^{2\pi i/p}$. Any function $f : A \to \mathbb{C}$ can be uniquely expressed as a linear combination of these χ_t; this change of basis is precisely the Fourier transform. When G is a nonabelian group, however, this same procedure cannot work: in particular, there are not enough homomorphisms of G into $\mathbb{C}$ to even span the space of all $\mathbb{C}$-valued functions on G. The representation theory of finite groups constructs the objects (invertible matrices) which can be used in place of the $\mathbb{C}$-valued homomorphisms above to develop a satisfactory theory of Fourier analysis over general groups.

Nonabelian Fourier transforms. We only discuss enough details of the theory to set down notation, and refer to [20] for a more complete exposition. A *representation* of a finite group G is a homomorphism $\rho : G \to \mathrm{U}(d)$, where $\mathrm{U}(d)$ denotes the group of unitary $d \times d$ matrices (with entries from $\mathbb{C}$); the dimension $d = d_\rho$ is referred to as the *dimension* of ρ. If $\rho : G \to \mathrm{U}(d)$ is a representation, a subspace W of $\mathbb{C}^d$ is said to be *invariant* if $\rho(g)(W) \subset W$ for all g. A representation is said to be *irreducible* if the only invariant subspaces are the trivial subspace $\mathbb{C}^d$ and $\{\vec{0}\}$.

For a function $f : G \to \mathbb{C}$ and an irreducible representation ρ, $\hat{f}(\rho)$ denotes *the Fourier transform of f at ρ* and is defined by

$$\hat{f}(\rho) = \sqrt{\frac{d_\rho}{|G|}} \sum_g f(g)\rho(g) \ .$$

Note that f takes values in $\mathbb{C}$ while ρ is matrix-valued. It is a fact that a finite group has a finite number of distinct irreducible representations (up to isomorphism), and the *Fourier transform* of a function $f : G \to \mathbb{C}$ is the collection of matrices $\hat{f}(\rho)$, taken over all distinct irreducible representations ρ.

Fixing a group G and a subgroup H, we shall focus primarily on the functions $\varphi_c : G \to \mathbb{C}$ of form

$$\varphi_c(g) = \begin{cases} \frac{1}{\sqrt{|H|}} & \text{if } g \in cH, \\ 0 & \text{otherwise,} \end{cases}$$

as these correspond to the states resulting from Step 3 above. The Fourier transform of such a function is then

$$\widehat{\varphi_c}(\rho) = \sqrt{\frac{d_\rho}{|G||H|}}\, \rho(c) \cdot \sum_{h \in H} \rho(h) \ .$$

Note, as above, that $\widehat{\varphi_c}(\rho)$ is a $d_\rho \times d_\rho$ matrix.

As H is a subgroup, it happens that $\sum_h \rho(h)$ is precisely $|H|$ times a projection operator (see, e.g., [10]); we write

$$\sum_h \rho(h) = |H|\, \pi_H(\rho) \ .$$

(The rank of $\pi_H(\rho)$ is determined by the number of copies of the trivial representation in the representation $\mathrm{Ind}_H^G \mathbf{1}$.) With this notation, we can express $\widehat{\varphi_c}(\rho)$ as $\sqrt{n_\rho}\, \rho(c) \cdot \pi_H(\rho)$ where $n_\rho = d_\rho |H|/|G|$. For a $d \times d$ matrix M, we let $\|M\|$ denote the matrix norm given by

$$\|M\|^2 = \mathbf{tr}\left(M^\dagger M\right) = \sum_{ij} |M_{ij}|^2 ,$$

where $M^\dagger$ denotes the conjugate transpose of M. Then the probability that we observe the representation ρ is

$$\begin{aligned} \|\widehat{\varphi_c}(\rho)\|^2 &= \left\|\sqrt{n_\rho}\, \rho(c)\pi_H(\rho)\right\|^2 \\ &= n_\rho \|\pi_H(\rho)\|^2 = n_\rho\, \mathbf{rk}\, \pi_H(\rho) \ , \end{aligned}$$

as $\rho(c)$ is unitary; here $\mathbf{rk}\, \pi_H(\rho)$ denotes the rank of the projection operator $\pi_H(\rho)$. See [10] for more discussion.

Since in this general setting Fourier transforms are matrix-valued, our Fourier sampling algorithm may require measurement of not just which representation we are in, but also the row and column.

In particular, Hallgren, Russell, and Ta-Shma [10] show that by measuring only the *names* of representations—the so-called *weak standard method* in the terminology of [7]—it is possible to reconstruct normal subgroups (and thus solve the HSP for *Hamiltonian groups*, all of whose subgroups are normal). More generally, this method reconstructs the *normal core* of a subgroup, i.e. the intersection of all its conjugates. On the other hand, they show that this is insufficient to solve Graph Automorphism, since even in an information-theoretic sense this method cannot distinguish between the trivial subgroup of S_n and most subgroups of order 2.

Grigni, Schulman, Vazirani and Vazirani [7] show that trivial and non-trivial subgroups are still information-theoretically indistinguishable, even if we do measure the rows and columns of the representation, under the assumption that a random basis is used for each representation. In other words, even the *strong standard method,* in which rows and columns are measured, cannot solve Graph Automorphism unless there exist bases for the representations of S_n with very special computational properties. (They also point out that since we can reconstruct normal subgroups, we can also solve the HSP for groups where the intersection of all normalizers (the Baer norm) has small index.)

Finally, recent work of Kuperberg [15] shows that for the HSP over the dihedral groups, consideration of the "plethysm basis" in the representation $\rho \otimes \sigma$, after independent observation of ρ and σ, can lead to a subexponential ($2^{O(\sqrt{n})}$) quantum circuit for the HSP. It is interesting to ask if this method gives similar speedups for the q-hedral and affine groups, discussed below.

Contributions of this paper. An important open question, then, is whether there are cases in which the *strong standard method* offers any advantage over a simple abelian transform or the *weak standard method.* In this paper, we settle this question in the affirmative. Our results deal primarily with the *q-hedral* groups, i.e., semidirect products of the form $\mathbb{Z}_q \ltimes \mathbb{Z}_p$, and in particular the *affine* groups $A_p \cong \mathbb{Z}_p^* \ltimes \mathbb{Z}_p$ where $q = p - 1$.

We begin in Section 2 by focusing on full reconstructibility. We define the *Hidden Conjugate Problem* as follows: given a group G, a non-normal subgroup H, and a function which is promised to be constant on the cosets of some conjugate bHb^{-1} of H (and distinct on distinct cosets), determine the subgroup bHb^{-1} by finding an element $c \in G$ so that $cHc^{-1} = bHb^{-1}$. We adopt the above classification (fully, information-theoretically, quantum information-theoretically) for this problem in the natural way. Then we show that given a subgroup of sufficiently small index, hidden conjugates in A_p are fully reconstructible (Theorem 2.1). This almost immediately implies that (for prime $q = (p-1)/\text{polylog}(p)$) subgroups of the q-hedral groups $\mathbb{Z}_p \ltimes Z_p$ are fully reconstructible (Theorem 2.2).

Moreover, our algorithms in Theorems 2.1 and 2.2 rely crucially on the high-dimensional representations of $\mathbb{Z}_q \ltimes \mathbb{Z}_p$, and we show in Section 4 that abelian methods (in other words, treating the group as a direct product rather than a semidirect one) do not suffice.

Section 3 concerns itself with information-theoretic reconstructibility. We generalize the results of Ettinger and Høyer on the dihedral group to the q-hedral groups and show that, assuming $q|(p-1)$, hidden conjugates are information-theoretically reconstructible in the q-hedral groups (Theorem 3.1). We then use this to show that under the same assumptions all subgroups are information-theoretically reconstructible as well (Theorem 3.2). In particular, the subgroups of the affine group are information-theoretically reconstructible.

We close in Section 5 by showing that the set of groups for which the HSP can be solved in polynomial time has the following closure property: if $\mathcal{H} = \{H_n\}$ is a family of groups for which we can efficiently solve the HSP and $\mathcal{K} = \{K_n\}$ is a family of groups for which $|K_n| = \text{polylog}|H_n|$, we can also efficiently solve the HSP for the family $\{G_n\}$, where each G_n is any extension of K_n by H_n. This subsumes the results of [10] on Hamiltonian groups, and also those of [12] on groups with commutator subgroups of polynomial size.

2 Full reconstructibility

Let A_p be the *affine group*, consisting of ordered pairs $(a, b) \in \mathbb{Z}_p^* \times \mathbb{Z}_p$, where p is prime, under the multiplication rule $(a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2, b_1 + a_1 b_2)$. A_p can be viewed as the set of affine functions $f_{(a,b)} : \mathbb{Z}_p \to \mathbb{Z}_p$ given by $f_{(a,b)} : x \mapsto ax + b$ where multiplication is given by function composition. Structurally, A_p is a semidirect product $\mathbb{Z}_p^* \ltimes \mathbb{Z}_p$. Its subgroups are as follows:

- Let $N \cong \mathbb{Z}_p$ be the normal subgroup of size p consisting of elements of the form $(1, b)$.
- Let H be the non-normal subgroup of size $p - 1$ consisting of the elements of the form $(a, 0)$. Its conjugates $H^b = (1, b) \cdot H \cdot (1, -b)$ consist of elements of the form $(a, (1-a)b)$. (In the action on $\mathbb{Z}_p$, H^b is the stabilizer of b.)
- More generally, if $a \in \mathbb{Z}_p^*$ has order q, let $N_a \cong \mathbb{Z}_q \ltimes \mathbb{Z}_p$ be the normal subgroup consisting of all elements of the form (a^t, b), and let H_a be the non-normal subgroup $H_a = \langle (a, 0) \rangle$ of size q. Then H_a consists of the elements of the form $(a^t, 0)$ and its conjugates $H_a^b = (1, b) \cdot H_a \cdot (1, -b)$ consist of the elements of the form $(a^t, (1 - a^t)b)$.

The representation theory of A_p. Construction of the representations of A_p requires that we fix a generator γ of $\mathbb{Z}_p^*$. Define $\phi : \mathbb{Z}_p^* \to \mathbb{Z}_{p-1}$ to be the isomorphism $\phi(\gamma^t) = t$. Let ω_p denote the pth root of unity $\mathrm{e}^{2\pi i/p}$. Then $A_p \cong \mathbb{Z}_p^* \ltimes \mathbb{Z}_p$ has $p-1$ one-dimensional representations σ_s given by $\sigma_t((a,b)) = \omega_{p-1}^{t\phi(a)}$, and one $(p-1)$-dimensional representation ρ given by

$$\rho((a,b))_{j,k} = \begin{cases} \omega_p^{bj} & k = aj \bmod p \\ 0 & \text{otherwise} \end{cases} \quad, \; 1 \le j,k < p \;,$$

where the indices i and j are elements of $\mathbb{Z}_p^*$. (The basis selected here is a Gel'fand-Tsetlin basis; see [16].) See [20, §8.2] for a more detailed discussion.

The affine group—and more generally, the q-hedral groups we discuss below—are *metacyclic* groups, i.e. extensions of a cyclic group $\mathbb{Z}_p$ by a cyclic group $\mathbb{Z}_q$. In [11], Høyer shows how to perform the (nonabelian) Fourier transform over such groups with a polynomial (i.e. polylog(p)) number of elementary quantum operations. (In fact, he does this only up to an overall phase factor, but this is sufficient for our purposes.)

Theorem 2.1. *Let p be prime. Then the hidden conjugates of H_a in $A_p = \mathbb{Z}_p^* \ltimes \mathbb{Z}_p$ are fully reconstructible if $(p-1)/|\langle a \rangle| = \mathrm{polylog}(p)$.*

Proof. Consider first the maximal non-normal subgroup $H = H_\gamma$ (where γ is a generator of $\mathbb{Z}_p^*$). Carrying out steps 1 through 3 of the Fourier sampling procedure outlined in the introduction results in a state over the group G which is uniformly supported on a random left coset of the conjugate $H^b = bHb^{-1}$. We now compute the quantum Fourier transform of this state according to the basis above. The associated projection operator is

$$\pi_{H^b}(\rho)_{j,k} = \frac{1}{p-1}\,\omega_p^{b(j-k)} \;,$$

for $1 \le j,k < p$. This is a circulant matrix of rank one. More specifically, every column is some root of unity times the vector

$$(u_b)_j = \frac{1}{p-1}\,\omega_p^{bj} \;,$$

$1 \le j < p$. This is also true of $\rho(c)\cdot\pi_{H^b}(\rho)$; since $\rho(c)$ has one nonzero entry per column, left multiplying by $\rho(c)$ simply multiplies each column of $\pi_{H^b}(\rho)$ by a phase. Note that in this case

$$n_\rho = d_\rho |H|/|G| = (p-1)/p = 1 - 1/p \;,$$

so that upon measurement the $(p-1)$-dimensional representation ρ is observed with overwhelming probability $1-1/p$. Assuming that we observe ρ, we can first carry out a partial measurement on the columns, and then transform the rows by left-multiplying $\rho(cH)$ by the quantum Fourier transform over $\mathbb{Z}_{p-1}$, $Q_{\ell,j} = (1/\sqrt{p-1})\,\omega_{p-1}^{-\ell j}$. This allows us to infer b by measuring the frequency ℓ. In particular, we observe a given value of ℓ with probability

$$P(\ell) = \left| \frac{1}{p-1} \sum_{j=1}^{p-1} \omega_p^{bj}\omega_{p-1}^{-\ell j} \right|^2 = \frac{1}{(p-1)^2} \left| \sum_{j=1}^{p-1} \mathrm{e}^{2i\theta j} \right|^2 = \frac{1}{(p-1)^2} \frac{\sin^2 (p-1)\theta}{\sin^2 \theta}$$

where

$$\theta = \left(\frac{b}{p} - \frac{\ell}{p-1} \right) \pi \;.$$

Now note that for any b there is an ℓ such that $|\theta| \le \pi/(2(p-1))$. Since

$$(2x/\pi)^2 \le \sin^2 x \le x^2$$

for $|x| \le \pi/2$, this gives $P(\ell) \ge (2/\pi)^2$.

Recall that the probability that we observed the $(p-1)$-dimensional representation ρ in the first place is $n_\rho = 1 - 1/p$. Thus if we measure ρ, the column, and then ℓ and then guess that b minimizes $|\theta|$, we will be right $\Omega(1)$ of the time. This can be boosted to high probability by repeating the experiment a polynomial number of times.

Consider now the more general case, when the hidden subgroup is a conjugate of the subgroup H_a where a's order q is a proper divisor of $p-1$. Recall that a given conjugate of H_a consists of the elements of the form $(a^t, (1-a^t)b)$. Then we have

$$\pi_{H_a^b}(\rho)_{j,k} = \frac{1}{q} \begin{cases} \omega_p^{b(j-k)} & k = a^t j \text{ for some } t \\ 0 & \text{otherwise} \end{cases} \;,$$

for $1 \le j,k < p$. In other words, the nonzero entries are those for which j and k lie in the same coset of $\langle a \rangle \subset \mathbb{Z}_p^*$. The rank of this projection operator is thus the number of cosets, which is the index $(p-1)/q$ of $\langle a \rangle$ in $\mathbb{Z}_p^*$. Since n_ρ is now q/p, we again observe ρ with probability

$$n_\rho \,\mathbf{rk}\, \pi_{H_a}(\rho) = (p-1)/p = 1 - 1/p \;.$$

Following the same procedure as before, we carry out a partial measurement on the columns of ρ, and then Fourier transform the rows. After changing the variable of summation from t to $-t$ and adding a phase shift of $\mathrm{e}^{-i\theta(p-1)}$ inside the $|\cdot|^2$, the probability we observe a frequency ℓ, assuming we find ourselves in the kth column, is

(2.1)

$$P(\ell) = \left| \frac{1}{\sqrt{q(p-1)}} \sum_{t=0}^{q-1} \omega_p^{b(a^t k \bmod p)} \omega_{p-1}^{-\ell(a^t k \bmod p)} \right|^2$$
$$= \frac{1}{q(p-1)} \left| \sum_{t=0}^{q-1} \mathrm{e}^{2i\theta(a^t k \bmod p)} \right|^2 \ .$$

Now note that the terms in the sum are of the form $\mathrm{e}^{i\phi}$ where (assuming w.l.o.g. that θ is positive)

$$\phi \in [-\theta(p-1), \theta(p-1)] \ .$$

If we again take ℓ so that $|\theta| \leq \pi/(2(p-1))$, then $\phi \in [-\pi/2, \pi/2]$ and all the terms in the sum have nonnegative real parts. We will obtain a lower bound the real part of the sum by showing that a constant fraction of the terms have $\phi \in (-\pi/3, \pi/3)$, and thus have real part more than $1/2$. This is the case whenever $a^t k \in (p/6, 5p/6)$, so it is sufficient to prove the following lemma:

Lemma 2.1. *Let a have order $q = p/\mathrm{polylog}(p)$ in $\mathbb{Z}_p^*$, p a prime. Then at least $(1/3 - o(1))q$ of the elements in the coset $\langle a \rangle k$ are in the interval $(p/6, 5p/6)$.*

Proof. We will prove this using *Gauss sums*, which quantify the interplay between the characters of $\mathbb{Z}_p$ and the characters of $\mathbb{Z}_p^*$. In particular, Gauss sums establish bounds on the distribution of powers of a. Specifically, if a has order q in $\mathbb{Z}_p^*$ then for any integer $k \not\equiv 0 \pmod p$ we have

$$\sum_{t=0}^{q-1} \omega_p^{a^t k} = \mathcal{O}(p^{1/2}) = o(p) \ .$$

(See [14] and Appendix A.)

Now suppose s of the elements x in $\langle a \rangle k$ are in the set $(p/6, 5p/6)$, for which $\mathrm{Re}\, \omega_p^x \geq -1$, and the other $q - s$ elements are in $[0, p/6] \cup [5p/6, p)$, for which $\mathrm{Re}\, \omega_p^x \geq 1/2$. Thus we have

$$\mathrm{Re} \sum_{t=0}^{q-1} \omega_p^{a^t k} \geq (q/2) - (3s/2).$$

If $s \leq (1/3 - \epsilon)q$ for any $\epsilon > 0$ this is $\Theta(q)$, a contradiction.

Now that we know that a fraction $1/3 - \epsilon$ of the terms in (2.1) have real part at least $1/2$ and the others have real part at least 0, we can take $\epsilon = 1/12$ (say) and write

$$P(\ell) \geq \frac{1}{q(p-1)} \left(\frac{q}{8} \right)^2 = \frac{1}{64} \frac{q}{p-1} = \frac{1}{\mathrm{polylog}(p)} \ .$$

Thus we observe the correct frequency with at least polynomially small probability; again this can be boosted to high probability by repetition.

We remark that the *q-hedral* groups $\mathbb{Z}_q \ltimes \mathbb{Z}_p$ embed naturally in $A_p \cong \mathbb{Z}_p^* \ltimes \mathbb{Z}_p$ (when $q \mid p-1$), and that the representation theory of these groups follows immediately from that of the affine groups (see below). In particular, if q is prime then H_a (as above) is the only non-normal subgroup of $\mathbb{Z}_q \ltimes \mathbb{Z}_p$ (where a is a generator of $\mathbb{Z}_q$) and the proof above implies that we can completely solve the Hidden Subgroup Problem for these groups. For instance, if q is a *Sophie Germain* prime, i.e. one for which $2q+1$ is also a prime, we can solve the HSP for $\mathbb{Z}_q \ltimes \mathbb{Z}_{2q+1}$. Thus, we have the following:

Theorem 2.2. *Let p and q be prime with $q = (p-1)/\mathrm{polylog}(p)$. Then subgroups of $\mathbb{Z}_q \ltimes \mathbb{Z}_p$ are fully reconstructible.*

3 Information-theoretic reconstructibility

We focus now on general q-hedral groups $\mathbb{Z}_q \ltimes \mathbb{Z}_p$, for generic values of q dividing $p-1$. As above, we consider the hidden conjugate problem for subgroups $H_a = \langle (a, 0) \rangle$. We will later patch these results together to obtain results for the full hidden subgroup problem over the affine groups. In this section we show that the conjugates of H_a are information-theoretically reconstructible. This generalizes the results of Ettinger and Høyer [3] who show this for the case $q = 2$, i.e. the dihedral groups.

Theorem 3.1. *Let p be prime and q a divisor of $p-1$. Then hidden conjugates in $\mathbb{Z}_q \ltimes \mathbb{Z}_p$ are information-theoretically reconstructible.*

Proof. The representations of $\mathbb{Z}_q \ltimes \mathbb{Z}_p$ include the q one-dimensional representations of $\mathbb{Z}_q$ given by $\sigma_\ell((a^t, b)) = \omega_q^{\ell t}$, $\ell \in \mathbb{Z}_q$ and $(p-1)/q$ distinct q-dimensional representations ρ_k given by

$$\rho_k((a^u, b))_{s,t} = \begin{cases} \omega_p^{k a^s b} & t = s + u \bmod q \\ 0 & \text{otherwise} \end{cases} \ ,$$

for each $0 \leq s, t < q$. Here k ranges over the elements of $\mathbb{Z}_p^*/\mathbb{Z}_q$, or, to put it differently, k takes values in $\mathbb{Z}_p^*$ but ρ_k and $\rho_{k'}$ are equivalent if k and k' are in the same coset of $\langle a \rangle$. These ρ_k are simply the $(p-1)/q$ diagonal blocks of the $(p-1)$-dimensional representation ρ of A_p.

Note that all conjugates of H_a lie in the (unique) subgroup isomorphic to $\mathbb{Z}_{q'} \ltimes \mathbb{Z}_p$, where q' is the order of a; thus without loss of generality we may assume that we are working with the largest non-normal subgroup H_a, where a is a generator of $\mathbb{Z}_q$.

Then summing ρ_k over the elements $(a^t, (1-a^t)b)$ gives the associated projection operator,

$$\left(\pi_{H_a^b}(\rho_k)\right)_{s,t} = (1/q)\ \omega_p^{k(a^s-a^t)b}$$

for $0 \le s, t < q$. This is again a matrix of rank 1, where each column (even after left multiplication by $\rho_k(c)$) is some root of unity times the vector $(u_k)_s = (1/q)\ \omega_p^{ka^s b}$. Note that $n_\rho = q/p$.

We now wish to show that there is a measurement whose outcomes, given two distinct values of b, have large $(1/\mathrm{poly}(n))$ total variation distance. First, we perform a series of partial measurements as follows: *(i.)* measure the name of the representation; *(ii.)* measure the column of the representation; and *(iii.)* perform a POVM with q outcomes, in each of which s is u or $u+1 \bmod q$ for some $u \in \mathbb{Z}_q$. The total probability we observe one of the q-dimensional representations, since there are $(p-1)/q$ of them, is $n_\rho(p-1)/q = 1 - 1/p$. Then these three partial measurements determine k, remove the effect of the coset, and determine that s has one of two values, u or $u+1$. Up to an overall phase we can write this as a two-dimensional vector

$$\frac{1}{\sqrt{2}}\begin{pmatrix} \omega_p^{ka^u b} \\ \omega_p^{ka^{u+1} b} \end{pmatrix} .$$

We now apply the Hadamard transform

$$\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

and measure s. The probability we observe u and $u+1$ is then $\cos^2\theta$ and $\sin^2\theta$ respectively, where $\theta = (\pi k a^u (a-1) b)/p$. Now when we observe a q-dimensional representation, the k we observe is uniformly distributed over $\mathbb{Z}_p^*/\mathbb{Z}_q$, and when we perform the POVM, the u we observe is uniformly distributed over $\mathbb{Z}_q$. It follows that the coefficient $m = ka^u(u-1)$ is uniformly distributed over $\mathbb{Z}_p^*$. For any two distinct b, b', the total variation distance is then

$$\frac{1}{2(p-1)} \sum_{m \in \mathbb{Z}_p^*} \left(\left| \cos^2 \frac{\pi m b}{p} - \cos^2 \frac{\pi m b'}{p} \right| + \left| \sin^2 \frac{\pi m b}{p} - \sin^2 \frac{\pi m b'}{p} \right| \right) .$$

This we rewrite

$$\begin{aligned} &\frac{1}{p-1} \sum_{m \in \mathbb{Z}_p} \left| \cos^2 \frac{\pi m b}{p} - \cos^2 \frac{\pi m b'}{p} \right| \\ &= \frac{1}{2(p-1)} \sum_{m \in \mathbb{Z}_p} \left| \cos \frac{2\pi m b}{p} - \cos \frac{2\pi m b'}{p} \right| \\ &\ge \frac{1}{4(p-1)} \sum_{m \in \mathbb{Z}_p} \left(\cos \frac{2\pi m b}{p} - \cos \frac{2\pi m b'}{p} \right)^2 \\ &= \frac{p}{4(p-1)} > \frac{1}{4} . \end{aligned}$$

(Adding the $m = 0$ term contributes zero to the sum in the second line. In the third line we use the facts that $|x| \le x^2/2$ for all $|x| \le 2$, the average of $\cos^2$ is $1/2$, and the two cosines have zero inner product.)

Since the total variation distance between any two distinct conjugates is bounded below by a constant, by standard results in probability theory we can distinguish between the p different conjugates with only $\mathcal{O}(\log p) = \mathrm{poly}(n)$ samples. Thus, hidden conjugates in q-hedral groups are information-theoretically reconstructible, completing the proof.

What remains to be seen is that in a group of the form $\mathbb{Z}_q \ltimes \mathbb{Z}_p$, where $q \mid p-1$, it is possible to determine the *order* of a hidden subgroup. Since there is a unique conjugacy class of subgroups of each order, given Theorem 3.1 we can (information-theoretically) reconstruct arbitrary hidden subgroups of $\mathbb{Z}_q \ltimes \mathbb{Z}_p$. Let H be a hidden subgroup of $\mathbb{Z}_q \ltimes \mathbb{Z}_p$ given by the oracle $f : \mathbb{Z}_q \ltimes \mathbb{Z}_p \to S$, and let $p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ be the prime factorization of q, in which case $k \le \sum_i \alpha_i = \mathcal{O}(\log q)$. For each $i \in [k]$ and $1 \le \alpha \le \alpha_i$, we will determine if $p_i^\alpha \mid |H|$. This suffices to determine $|H|$, at which point the subgroup H can be determined by Theorem 3.1.

THEOREM 3.2. *Let p be prime and q a divisor of $p-1$. The subgroups of the q-hedral groups $\mathbb{Z}_q \ltimes \mathbb{Z}_p$ are information-theoretically reconstructible. In particular, the subgroups of the affine groups $A_p = \mathbb{Z}_p^* \ltimes \mathbb{Z}_p$ are information-theoretically reconstructible.*

Proof. By initially applying the techniques of [10] (the weak standard method), we may (fully) reconstruct H if H is a non-trivial normal subgroup. (This follows because these particular semidirect product groups have the special property that if A is a non-trivial normal subgroup and $A \subset B$, then B is normal; in particular, the normal core

$$\bigcap_{\gamma \in G} \gamma C \gamma^{-1}$$

of any non-normal subgroup C is the identity group.) It remains to consider non-normal subgroups H. Recall that in this case, H is cyclic and $|H|$ is equal to the order of a, where $H = \langle (a,b) \rangle$. Now, for each $i \in [k]$ and $1 \le \alpha \le \alpha_i$, let $\Upsilon_i^\alpha : \mathbb{Z}_q \ltimes \mathbb{Z}_p \to \mathbb{Z}_{q/p_i^\alpha}$ be the homomorphism given by

$$\Upsilon_i^\alpha : (a,b) \mapsto a^{p_i^\alpha} \quad .$$

Then let

$$A_i^{\alpha_i} = \ker \Upsilon_i^\alpha = \{\gamma \in \mathbb{Z}_q \ltimes \mathbb{Z}_p \mid \gamma^{p_i^{\alpha_i}} = \mathbf{1}\} \ ,$$

where $\mathbf{1}$ denotes the identity element of $\mathbb{Z}_q \ltimes \mathbb{Z}_p$. $A_i^{\alpha_i}$ is the subgroup of $\mathbb{Z}_q \ltimes \mathbb{Z}_p$ consisting of all elements whose orders are a multiple of p_i^α. Consider now the function

$$(f, \Upsilon_i^\alpha) : \mathbb{Z}_q \ltimes \mathbb{Z}_p \to S \times \mathbb{Z}_{q/p_i^\alpha}$$

given by $(f, \Upsilon_i^\alpha)(\gamma) = (f(\gamma), \Upsilon_i^\alpha(\gamma))$. Observe that (f, Υ_i^α) is constant (and distinct) on the left cosets of $H \cap A_i^\alpha$ and, furthermore, the subgroup $H \cap A_i^\alpha$ has order p^α if and only if p^α divides the order of a. We may then determine if $H \cap A_i^\alpha$ has order p^α by assuming that it does, applying the result of Theorem 3.1, and checking the result against the original oracle f. This allows us to determine the prime factorization of $|H|$, as desired. Therefore, all subgroups of the q-hedral groups $\mathbb{Z}_q \ltimes \mathbb{Z}_p$ are information-theoretically reconstructible.

As in the dihedral case [3], we know of no polynomial-time algorithm which can reconstruct the most likely b from these queries.

4 Failure of the abelian Fourier transform

In [3] the abelian Fourier transform over $\mathbb{Z}_2 \times \mathbb{Z}_p$ is used in a reconstruction algorithm for the dihedral groups. Using this sort of "forgetful" abelian Fourier analysis it is similarly information-theoretically possible to reconstruct subgroups of the q-hedral groups, when q is small enough.

However, it does not seem possible to reconstruct subgroups of A_p using the abelian Fourier transform over the direct product $\mathbb{Z}_p^* \times \mathbb{Z}_p$. Let us consider the hidden conjugate problem for H, i.e., H_a where a is a generator of $\mathbb{Z}_p^*$.

If a is a generator, the characters of $\mathbb{Z}_p^* \times \mathbb{Z}_p$ are simply $\rho_{k,\ell}(a^t, b) = \omega_{p-1}^{kt} \omega_p^{\ell b}$. Summing these over $H_a = \{(a^t, (1-a^t)b\}$ shows that we observe the character (k, ℓ) with probability

$$\begin{aligned} P(k,\ell) &= \frac{1}{p\,(p-1)^2} \left| \sum_{t \in Z/(p-1)} \omega_{p-1}^{kt} \omega_p^{\ell(1-a^t)b} \right|^2 \\ &= \frac{1}{p\,(p-1)^2} \left| \sum_{x \in \mathbb{Z}_p^*} \omega_{p-1}^{k \log_a x} \omega_p^{-\ell x b} \right|^2 \quad . \end{aligned}$$

This is the inner product of a multiplicative character with an additive one, which is another Gauss sum. In particular, assuming $b \neq 0$, we have

$$\begin{aligned} P(0,0) &= 1/p \\ P(0,\ell \neq 0) &= 1/(p\,(p-1)^2) \\ P(k \neq 0, 0) &= 0 \\ P(k \neq 0, \ell \neq 0) &= 1/(p-1)^2 \end{aligned}$$

(see Appendix A). Since these probabilities don't depend on b, the different conjugates H_a^b with $b \neq 0$ are indistinguishable from each other. Thus it appears essential to use the nonabelian Fourier transform and the high-dimensional representations of A_p.

5 Closure under extending small groups

In this section we show that for any polynomial-size group K and any H for which we can solve the HSP, we can also solve the HSP for any extension of K by H. (Note that this is more general than split extensions, i.e. semidirect products $H \ltimes K$.) This includes the case discussed in [10] of Hamiltonian groups, since all such groups are direct products (and hence extensions) by abelian groups of the quaternion group Q_8 [19]. It also includes the case discussed in [5] of groups with commutator subgroups of polynomial size, such as extra-special p-groups, since in that case $K = G'$ and $H \cong G/G'$ is abelian. Indeed, our proof is an easy generalization of that in [5].

Theorem 5.1. *Let H be a group for which hidden subgroups are fully reconstructible, and K a group of polynomial size in $\log|H|$. Then hidden subgroups in any extension of K by H, i.e. any group G with $K \lhd G$ and $G/K \cong H$, are fully reconstructible.*

Proof. We assume that G and K are encoded in such a way that multiplication can be carried out in classical polynomial time. We fix some transversal $t(h)$ of the left cosets of K. First, note that any subgroup $L \subseteq G$ can be described in terms of i) its intersection $L \cap K$, ii) its projection $L_H = L/(L \cap K) \subseteq H$, and iii) a representative $\eta(h) \in L \cap (t(h) \cdot K)$ for each $h \in L_H$. Then each element of L_H is associated with some left coset of $L \cap K$, i.e. $L = \bigcup_{h \in L_H} \eta(h) \cdot (L \cap K)$. Moreover, if S is a set of generators for $L \cap K$ and T is a set of generators for L_H, then $S \cup \eta(T)$ is a set of generators for L.

We can reconstruct S in classical polynomial time simply by querying the function h on all of K. Then $L \cap K$ is the set of all k such that $h(k) = h(1)$, and we construct S by adding elements of $L \cap K$ to it one at a time until they generate all of $L \cap K$.

To identify L_H, as in [5] we define a new function h' on H consisting of the unordered collection of the values of h on the corresponding left coset of K:

$$h'(h) = \{h(g) \mid g \in t(h) \cdot K\}.$$

Each query to h' consists of $|K| = \mathrm{poly}(n)$ queries to h. The level sets of h' are clearly the cosets of L_H, so we reconstruct L_H by solving the HSP on H. This yields a set T of generators for L_H.

It remains to find a representative $\eta(h)$ in $L \cap (t(h) \cdot K)$ for each $h \in T$. We simply query $h(g)$ for all $g \in t(h) \cdot K$, and set $\eta(h)$ to any g such that $h(g) = h(1)$. Since $|T| = \mathcal{O}(\log |H|) = \mathrm{poly}(n)$ this can be done in polynomial time, completing the proof.

□

Unfortunately, we cannot iterate this construction more than a constant number of times, since doing so would require a superpolynomial number of queries to h for each query of h'. If K has superpolynomial size it is not clear how to obtain $\eta(h)$, even when H has only two elements: this is precisely the difficulty with the dihedral group.

References

[1] Robert Beals. Quantum computation of Fourier transforms over symmetric groups. In ACM, editor, *Proceedings of the twenty-ninth annual ACM Symposium on the Theory of Computing*, pages 48–53, El Paso, Texas, 4–6 May, 1997. ACM Press.

[2] Ethan Bernstein and Umesh Vazirani. Quantum complexity theory (preliminary abstract). In *Proceedings of the Twenty-Fifth Annual ACM Symposium on the Theory of Computing*, pages 11–20, San Diego, California, 16–18 May 1993.

[3] Mark Ettinger and Peter Høyer. On quantum algorithms for noncommutative hidden subgroups. Technical Report quant-ph/9807029, Quantum Physics e-Print Archive, 1998.

[4] Mark Ettinger and Peter Høyer and Emmanuel Knill. Hidden subgroup states are almost orthogonal. Technical Report quant-ph/9901034, Quantum Physics e-Print Archive, 1999.

[5] Katalin Friedl, Gábor Ivanyos, Frédéric Magniez, Miklos Santha, and Pranab Sen. Hidden translation and orbit coset in quantum computing. Technical Report quant-ph/0211091, Quantum Physics e-Print Archive, 2002.

[6] William Fulton and Joe Harris. *Representation Theory: A First Course*. Number 129 in Graduate Texts in Mathematics. Springer-Verlag, 1991.

[7] Michelangelo Grigni, Leonard J. Schulman, Monica Vazirani, and Umesh Vazirani. Quantum mechanical algorithms for the nonabelian hidden subgroup problem. In *Proceedings of the 33rd ACM Symposium on Theory of Computing*, pages 68–74, 2001.

[8] Lisa Hales and Sean Hallgren. Quantum fourier sampling simplified. In *Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing*, Atlanta, Georgia, 1–4 May 1999.

[9] Lisa Hales and Sean Hallgren. An improved quantum fourier transform algorithm and applications. In *41st Annual Symposium on Foundations of Computer Science*. IEEE, 2000.

[10] Sean Hallgren, Alexander Russell, and Amnon Ta-Shma. Normal subgroup reconstruction and quantum computation using group representations. In *Proceedings of the 32nd ACM Symposium on Theory of Computing*, pages 627–635, 2000.

[11] Peter Høyer. Efficient quantum transforms. Technical Report quant-ph/9702028, Quantum Physics e-Print Archive, 1997.

[12] Gábor Ivanyos, Frédéric Magniez, and Miklos Santha. Efficient quantum algorithms for some instances of the non-abelian hidden subgroup problem. Technical Report quant-ph/0102014, Quantum Physics e-Print Archive, 2001.

[13] Richard Jozsa. Quantum factoring, discrete logarithms and the hidden subgroup problem. Technical Report quant-ph/0012084, Quantum Physics e-Print Archive, 2000.

[14] Sergei V. Konyagin and Igor E. Shparlinski. *Character sums with exponential functions and their applications*. Number 136 in Cambridge Tracts in Mathematics. Cambridge University Press, Cambridge, 1999.

[15] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. Technical Report quant-ph/0302113, Quantum Physics e-Print Archive, 2003.

[16] Cristopher Moore, Daniel Rockmore, Alexander Russell, and Leonard Schulman. Generic quantum Fourier transforms. In *Proceedings of the 15th Annual ACM-SIAM Symposium on Discrete Algorithms*, New Orleans, LA, 11–13 January 2004.

[17] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. Number 20 in Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.

[18] Martin Roetteler and Thomas Beth. Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups. Technical Report quant-ph/9812070, Quantum Physics e-Print Archive, 1998.

[19] Joseph Rotman. *An Introduction to the Theory of Groups*. Number 148 in Graduate Texts in Mathematics. Springer-Verlag, 1994.

[20] Jean-Pierre Serre. *Linear Representations of Finite Groups*. Number 42 in Graduate Texts in Mathematics. Springer-Verlag, 1977.

[21] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[22] Daniel R. Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, October 1997.

Acknowledgements. We are grateful to Wim van Dam, Frederic Magniez, Martin Rötteler, and Miklos Santha for helpful conversations, and to Sally Milius and Tracy Conrad for their support. Support for this work was provided by the California Institute of Technology's Institute for Quantum Information (IQI), the Mathematical Sciences Research Institute (MSRI), the Institute for Advanced Study (IAS), NSF grants ITR-0220070, ITR-0220264, CCR-0093065, EIA-0218443, QuBIC-0218563, the Charles Lee Powell Foundation, and the Bell Fund.

A Notes on exponential sums

The basic *Gauss sum* bounds the inner products of additive and multiplicative characters of $\mathbb{F}_p$, the finite field of prime cardinality p. Definitive treatments appear in [17, §5] and [14]. Considering $\mathbb{F}_p$ as an additive group with p elements, we have p additive characters $\chi_s : \mathbb{F}_p \to \mathbb{C}$, for $s \in \mathbb{F}_p$, given by $\chi_s : z \mapsto \omega_p^{sz}$, where, as above, $\omega_p = \mathrm{e}^{2\pi i/p}$ is a primitive pth root of unity. Likewise considering the elements of $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$ as a multiplicative group, we have $p-1$ characters $\psi_t : \mathbb{F}_p^* \to \mathbb{C}$, for $t \in \mathbb{F}_p^*$, given by $\psi_t : g^z \mapsto \omega_{p-1}^{tz}$, where $\omega_{p-1} = \mathrm{e}^{2\pi i/(p-1)}$ is a primitive $(p-1)$th root of unity and g is a multiplicative generator for the (cyclic) group $\mathbb{F}_p^*$.

With this notation the basic Gauss sum is the following:

Theorem A.1. *Let χ_s be an additive character and ψ_t a multiplicative character of $\mathbb{F}_p$. If $s \neq 0$ and $t \neq 1$ then*

$$\Big|\sum_{z\in\mathbb{F}_p^*} \chi_s(z)\,\psi_t(z)\Big| = \sqrt{p}.$$

Otherwise

$$\sum_{z\in\mathbb{F}_p^*} \chi_s(z)\psi_t(z) = \begin{cases} p-1 & \text{if } s=0, t=1,\\ -1 & \text{if } s=0, t\neq 1,\\ 0 & \text{if } s\neq 0, t=1.\end{cases}$$

See [17, §5.11] for a proof.

This basic result has been spectacularly generalized. In the body of the paper we require bounds on additive characters taken over multiplicative subgroups of $\mathbb{F}_p^*$. Such sums are discussed in detail in [14]. The specific bound we require is the following.

Theorem A.2. *Let χ_t be a nontrivial additive character of $\mathbb{F}_p$ and $a \in \mathbb{F}_p^*$ an element of multiplicative order q. Then*

$$\sum_{z=0}^{q-1} \chi_t(a^z) = \begin{cases} \mathcal{O}(p^{1/2}), & \text{if } q \geq p^{2/3},\\ \mathcal{O}(p^{1/4}q^{3/8}), & \text{if } p^{1/2} \leq q \leq p^{2/3},\\ \mathcal{O}(p^{1/8}q^{5/8}), & \text{if } p^{1/3} \leq q \leq p^{1/2}.\end{cases}$$

See [14, §2] for a proof.

Note that in the body of the paper, we use $\mathbb{Z}_p$ to denote the additive group of integers modulo p and $\mathbb{Z}_p^*$ to denote the multiplicative group of integers modulo p.